1   <u>**REMARKS**</u>

2   These remarks follow the order of the paragraphs of the office action. Relevant portions of the

3   office action are shown indented and italicized.

4   *DETAILED ACTION*

5   *Response to Arguments*

6   *Applicant's arguments filed November 28, 2005 have been fully considered but are not*

7   *found persuasive in view of the ground(s) of rejection set forth below.*

8   *As address below, the claim 1 is anticipated by S. Ma, et al. "EventMiner: An*

9   *integrated mining tool for Scalable Analysis of Event Data", May 21, 2001,*

10   *www.research.ibm.com.*

11   *Applicant argues that applicant's apparatus and system for monitoring events in*

12   *a computer network enabling an operator of an intrusion-detection system to*

13   *simultaneously monitor various event attributes versus the arrival time of the events.*

14   *However, "the apparatus and system... to simultaneously monitor various event*

15   *attributes" cannot be found as a claim limitation in the claim 1 because the claim 1 only*

16   *recites the viewing of the primary attribute and the multiple attribute values of the*

17   *primary attribute are viewed on the same display. Nowhere in the claim 1 recites a*

18   *secondary attribute being viewed together with the primary attribute on the same display.*

19   *Although multiple attribute values related to the primary attribute can be presented on*

20   *the same display, there is a fundamental difference between the attribute values for one*

21   *attribute and the attribute values for another attribute. Moreover, it is not ascertained*

22   *from the claim invention set forth in the claim 1 whether the claim limitation of*

23   *"attributes" refer to event attributes, pattern attributes or the data attributes. Applicant*

24   *failed to particularly point out and distinctly claim the subject matter which applicant*

25   *regards as invention.*

26   *Applicant also argues that there is apparently no indication that Ma performs a*

27   *step of determining a primary attribute" as in claim 1. However, the cited prior art*

28   *teaches in Fig. 7 and the last paragraph of the Page 12 plotting the primary attribute*

29   *(e.g., with the attribute values indicating the troublesome hosts having significantly high*

30   *event counts) versus time with the attribute values for events in a communication network*

31   *and the primary attribute is selected from a plurality of attributes related to the one or*

32   *more significant measurements such as the co- occurrences (i.e., the total number of*

33   *times that two hosts generate events within a predefined time window), the conditional*

34   *probability of the two hosts (i.e., the probability of a host generating an event given the*

35   *observation that the other host has generated an event), the chi- squared test and so on.*

36   *Fig. 4 shows the coloring of the events having the primary attribute with the patterns*

37   *indicating the authentication failure and SNMP request in order to differentiate using the*

38   *coloring the events with authentication failure from other events. A pattern label is*

39   *assigned to the events falling into the same pattern. Finally, the operator can view*

40   *different event <u>attributes</u> by switching menus (Fig. 6).*

41   *Applicant argues that, "the cited reference. S. Ma, et al., indeed presents other*

42   *event mining methods. That visualization method using a two-dimensional mapping*

43   *technique of arbitrary event attributes versus arrival time enabling an operator to*

44   *analyze the event history. A distinct disadvantage of this method is that only one of the*

event attributes may be plotted versus the arrival time of the events. Thus, the operators have to switch continuously between the various event attributes to make sure that they do not miss a significant event pattern. The disadvantages of S. Ma et al., are overcome with the invention claimed in claims 1-15. The Examiner respectfully disagrees with the applicant's remarks because applicant's statement, "only one of the event attributes maybe plotted versus arrival time of the events", is incorrectly construed. As previously addressed, Ma has taught in Fig. 7 and the last paragraph of the Page 12 plotting the primary attribute (e.g., with the attribute values indicating the troublesome hosts having significantly high event counts) versus time with the attribute values for events in a communication network. Ma has also taught a plurality of attributes related to the one or more significant measurements such as the co-occurrences (i.e., the total number of times that two hosts generate events within a predefined time window), the conditional probability of the two hosts (i.e., the probability of a host generating an event given the observation that the other host has generated an event), the chi-squared test and so on wherein the attribute values are plotted in the same plot, it is clear that Ma discloses attributes including categorical attributes of the hosts, event types, severity of the events, etc. See Figs. 2,6,7 and 9.

Applicant's statement, "the operators have to switch continuously between the various event attributes to make sure that they do not miss a significant event pattern," is incorrect. This is because in Ma many significant event patterns are simultaneously identified within a single plot without the operator's switching between the various event attributes.

Applicant argues that, "although Ma has a display, Ma apparently do not allocate a display label to the events indicating the attribute values of the primary attribute." It is noted that the claim 1 requires "a display label to the events indicating the attribute values of the primary attribute." However, Ma discloses display label to the events such as "Link down of host A", "node down of host B", "authentication failure of host A", etc., including the colors for coloring the different patterns that indicate the attribute values of the primary attribute such as the co- occurrences of some specific events within a predefined time window.

Applicant also argues that, "although Ma has a display, Ma apparently do not have a second display." This argument does not make sense, because the claim 1 set forth "a second display label" which is different from the meaning of "a second display." Applicant's claim 1 recites "a second display label". However, Ma discloses display label including the colors for coloring the different patterns for the events in the communication network that indicate the attribute values of the primary attribute such as the co-occurrences of some specific events within a predefined time window.

Claim Rejections - 35 USC5 102
The following is a quotation of the appropriate paragraphs of 36 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

 A person shall be entitled to a patent unless —

  (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale this country, more than one year prior to the date of application for patent in the United States.

Application/Control Number: 10/798,070   14/28

1   _Claims 1-20 are rejected under 35 U.S.C. 102(b)_ as being anticipated by S. Ma, et al.,

2   "EventMiner: An integrated mining tool for Scalable Analysis of Event Data", May 21,

3   2001, _www.research.ibm.com_

4

5   In response, applicants respectfully state that exception is taken with the so called equivalencies

6   of elements in _Claims 1-20_ and the cited art. This is in regard to use of words in claims 1-20 of

7   'attributes', 'primary', 'events', 'display label' etc. Thus, the present invention is not anticipated

8   by S. Ma, et al. The present invention provides methods for monitoring events in a computer

9   network, said computer network triggering said events, wherein each event is provided with

10   attribute values allocated to a given set of attributes. It provides methods, apparatus and systems

11   for monitoring events in a computer network enabling an operator of an intrusion-detection

12   system to simultaneously monitor various event attributes versus the arrival time of the events

13

14   The cited art to Ma, filed: May 21, 2001, is entitled, "EventMiner: An integrated mining tool for

15   Scalable Analysis of Event Data". Its abstract reads, "Exploring large data sets typically involves

16   activities that interwoven the following: querying databases, mining the results returned, and

17   visualizing both the raw data and the parterres discovered. This interweaving of functions arises

18   both from the semantics of what the analyst hopes to achieve and from salability requirements for

19   dealing with large data volumes. Herein is described a tool, EventMiner, that integrates querying

20   mining , and visualization so as to better analyze temporal data. We discuss the novel

21   visualization techniques employed such as visualizing the results of data mining. Also, we

22   address the large scale visualization of categorical data and how intelligent ordering of data can

23   aid in this task. Through out, ..." _This is apparently not the invention in claims 1-20._

24

25   _Claim 1: Ma teaches a method of monitoring events in a computer network, the method_
26   _comprising: Said computer network triggering said events, each event being provided_
27   _with attribute values allocated to a given set of attributes (The term "attributes" ore not_
28   _clear as it may be related to the data object attributes for each event or the pattern_
29   _attributes for each pattern for a plurality of data objects; However, the pattern attributes_
30   _for a plurality of data objects are also related to the data object attributes am a pattern is_
31   _computed from the plurality of data objects. The cited reference teach mapping a_
32   _plurality of data attributes to item to identify correlations across different hosts and event_
33   _types by using the mapping that maps the pair of event type and host name to item and_
34   _leaves key empty. See Page 11. Moreover the cited reference in Page 1, second_

Application/Control Number: 10/798,070   **15/28**

paragraph, explicitly teaches the attribute values, see the last paragraph of Page 6 and the first and second paragraphs of Page 8, the last paragraph of Page 12 and **the real data set** collected from a production computer network containing thousands of managed nodes including routers hubs and servers are described in the last paragraph of page 3 and identifying unknown event patterns that can be used for real-time monitoring is described in the second paragraph of page 3. Ma has also **taught a plurality of pattern attributes related to the one or more significant measurements such as the co-occurrences**, i.e. the total number of times that two hosts generate events within a predefined time window, the conditional probability of the two hosts, i.e., the probability of a host generating an event given the observation that the other host has generated an event, the chi-squared test and so on);

Providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting a time period and the y-axis present an attribute value range (e.g., The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and leaves key empty. See Page 11. Figs. 2, 4, 6, 7, 9 and the third paragraph of Page 8 describes a scatter plot or cross plot having any-axis representing around 160 hosts of a communication network and the x axis has been described in the figures as well as the first paragraph of page 6; for attribute value range, see these figures as well as the description in the second paragraph of Page 8);

Determining a primary attribute of the events selected from the given set of attributes to be presented with its attribute values on the y-axis of the cross plot (e.g., The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and leaves key empty. The attributes including the categorical attributes or temporal attributes and the primary attribute values are displayed in Figs. 2, 4, 6 and 7 and multiple attributes are described in the last paragraphs of Page 11 and 12).

Allocating a first display label (e.g., one of the colors indicating the patterns such as the Pattern 1, Pattern 2, Pattern 3, and Pattern 4 as marked in the scatter plot or the cross plot of Figs. 2, 6, 7 and 9 such as "Link down of host A" and "node down of host B") to the events (e.g. alarms in Page 10) indicating (mapping of the attributes wherein the mapping results are shown in the plots with the patterns identifying/indicating the attribute values of the primary attribute related to the categorical attribute such as the host A or the host B. Moreover, the pattern attribute values identifying the pattern 1 and the pattern 2 also describe the primary attribute such as the host A and the host B for the patterns such as "Link down of host A " and "node down of host B") the attribute values of the primary attribute (e.g., co-occurrence of certain events or the categorical attribute and event type associated with the events wherein the primary attribute is related to the primary attribute of the data set or the primary attribute of the patterns; See Page 12 and the key attribute values are described in the second paragraph of page 3), providing a pattern algorithm (the pattern algorithm is described in Fig. 7 as well as the mining algorithm as described in the last paragraph of page 12 or the Event Miner for ordering categorical values wherein the event generating, say every 300 seconds, may be identified) to detect whether an arrived event (arrived event are the selected event objects

Application/Control Number: 10/798,070   16/28

1   *or the selected data objects in a specific time range related to the events progressively*
2   *loaded from a database or the mining alarm logs in a real time system; see first*
3   *paragraph of page 13 and the last paragraph of page 10 and a new query that retrieves*
4   *the relevant data objects for more analysis in which a new query is restricted to a range*
5   *constraint for a numerical attribute; see the last paragraph of page 10) is part of the*
6   *given pattern (is part of the given pattern such as the Pattern 1 or the Pattern 2 from the*
7   *identifiable patterns such as the SNMP request, authentication failure link up, link*
8   *down, port up, port down wherein authentication failure indicates a possible security*
9   *intrusion and link down of host A indicates the attribute associated with the data objects*
10 *as well as the attribute associated with the event) on the basis of a comparison of the*
11 *attributes allocated to the given pattern and of the attributes assigned to the arrived event*
12 *(e.g., the co-occurrence measurements for events can be computed for the data sets or the*
13 *data objects and the temporal correlation with the selected hosts from the other side of*
14 *the AttributeViewer can be identified using the color linkage by the coloring and filtering*
15 *algorithm or the data mining algorithm in which the difference or similarity in terms of*
16 *patterns indicated by colors is compared; see page 12-13), providing a mapping*
17 *algorithm to map any attribute value of an attribute selected from the given set of*
18 *attributes onto the y-axis of the cross plot (see the last paragraphs of Page 11-12; The*
19 *cited reference teach napping a plurality of data attributes to item to identify correlations*
20 *across different hosts and event types by using the mapping that maps the pair of event*
21 *type and host name to item and leaves key empty.).*
22   *Allocating a second display label (e.g., one of the colors indicating the patterns*
23 *such as the Pattern 1. Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or*
24 *the cross plot of Figs. 2, 6, 7; SNMP request, authentication failure, link up, link down,*
25 *port up, port down wherein authentication failure indicates a possible security intrusion*
26 *may be used as display labels as well The attribute values may he used as display labels*
27 *as well) to the events indicating the attribute values of the attributes being uncovered*
28 *(discovered) as part of the given pattern (e.g.. the co-occurrence measurements for events*
29 *can be computed and the temporal correlation with the selected hosts from the other side*
30 *of the AttributeViewer can be identified using the color linkage by the coloring and*
31 *filtering algorithm or the data mining algorithm in which the difference or similarity in*
32 *terms of patterns indicated by colors is compared; see page 12-13; the display labels*
33 *indicate the attribute values of the attributes being discovered as part of the given*
34 *pattern, for example, the second host was near a critical level for a key metric indicates*
35 *the attribute values of the attributes being discovered as part of the given pattern),*
36 *plotting all the events arrived within the time period and including an attribute value*
37 *allocated to the primary attribute into the cross plot with the first display label indicating*
38 *the primary attribute, the position of the first display label of each event in the cross plot*
39 *being determined on the basis of the attribute value of the primary attribute of the event*
40 *and its arrival time (e.g., The cited reference teach mapping a plurality of data attributes*
41 *to item to item identify correlations across different hosts and event types by using the*
42 *mapping that maps the pair of event type and host name to item and leaves key empty.*
43 *Figs. 2, 4, 6, and 7 and the related paragraphs mentioned above in "allocating a first*
44 *display label", e.g., one of the colors indicating the patterns such as the Pattern 1,*
45 *Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or the cross plot of Figs.*

Application/Control Number: 10/798,070 **17/28**

1   2, 6, 7; SNMP request, authentication failure, link up, link down, port up, port down
2   wherein authentication failure indicates a possible security intrusion may be used as
3   display labels as well. The attribute values may be used as display labels as well), and.
4   Plotting the all events arrived within the time period (Figs. 2, 4, 6, and 7 plot the
5   all events within a specific time range) and being detected by means of the pattern
6   algorithm (by the event miner algorithm) as pail of the given pattern into the cross plot
7   with the second display label (e.g., one of the colors indicating the patterns such as the
8   Pattern 1, Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or the cross
9   plot of Figs. 2, & 7 and 9 or Pattern 2 or the Green Spike in Fig. 10), the position of the
10   second display label of each event in the cross plot being determined by the mapping
11   algorithm on the basis of the attribute value of the attribute of the event (see Figs. 1-10)
12   on the basis of the attribute value of the attribute of the event being uncovered
13   (uncovered for example in the alarm log and uncovered by the mining algorithm) as part
14   of the given pattern and its arrival time (discovered as part of the given pattern such as
15   Patterns 1-4 and its arrival time; all the selected events are in a specific time range as
16   plotted in Figs.2, 4, 6, 7 and 10).
17   In other words, Ma discloses an apparatus and system for monitoring events in a
18   computer network enabling an operator of an intrusion-detection system to
19   simultaneously monitor various event attributes versus the arrival time of the events, for
20   example, authentication failure indicates a possible security intrusion may be used as
21   display labels. The cited prior alt teaches in Fig. 7 and the last paragraph of the Page 12
22   plotting the primary attribute (e.g., with the attribute values indicating the troublesome
23   hosts having significantly high event counts) versus time with the attribute values for
24   events in a communication network and the primary attribute for a host is selected from a
25   plurality of attributes related to the categorical values, the one or more significant
26   measurements such as the co-occurrences (i.e., the total number of times that two hosts
27   generate events within a predefined time window), the conditional probability of the two
28   hosts (i.e., the probability of a host generating an event given the observation that the
29   other host has generated an event), the chi-squared test end so on.
30   Fig. 4 shows the coloring of the events having the primary attribute with the
31   patterns indicating the authentication failure and SNMP request in order to differentiate
32   using the coloring the events with authentication failure from other events. A pattern
33   label is assigned to the events falling into the same pattern. Finally, the operator can
34   view different event attributes by switching menus (Fig. 6).
35   Ma has taught in Fig. 7 and the last paragraph of the Page 12 plotting the
36   primary attribute (e.g., with the attribute values indicating the troublesome hosts having
37   significantly high event counts) versus time with the attribute values for events in a
38   communication network. Ma has also taught a plurality of attributes related to the one or
39   more significant measurements such as the co-occurrences (i.e., the total number of times
40   that two hosts generate events within a predefined time window), the conditional
41   probability of the two hosts (i.e., the probability of a host generating an event given the
42   observation that the other host has generated an event), the chi-squared test and so on
43   wherein the attribute values are plotted in the same plot. See Figs. 2, 6, 7 and 9. Many
44   significant event patterns are simultaneously identified within a single plot without the
45   operator's switching between the various event attributes.

Application/Control Number: 10/798,070   18/28

1   *Ma discloses display label including the colors for coloring the different patterns*
2   *that indicate the attribute values of the primary attribute such as the co-occurrences of*
3   *some specific events within a predefined time window.*
4

5   In response, applicants respectfully state that claim 1 is amended to better clarify the claimed
6   invention. Claim 1 as amended reads,

7

8   1. A method of monitoring events in a computer network, the method comprising:
9

10   said computer network triggering said events, each event being provided with attribute
11   values allocated to a given set of attributes of said each event,
12

13   simultaneously monitoring various event attributes versus the arrival time of each the
14   events,
15

16   providing an event display with a cross plot having x and y coordinate axes, the x-axis
17   presenting a time period and the y-axis presenting an attribute value range,
18

19   determining a primary attribute of the events selected from the given set of attributes to
20   be presented with its attribute values on the y-axis of the cross plot,
21

22   allocating a first display label to the events indicating the attribute values of the primary
23   attribute, providing a pattern algorithm to detect whether an arrived event is part of the
24   given pattern on the basis of a comparison of the attributes allocated to the given pattern
25   and of the attributes assigned to the arrived event, providing a mapping algorithm to map
26   any attribute value of an attribute selected from the given set of attributes onto the y-axis
27   of the cross plot,
28

29   allocating a second display label to the events indicating the attribute values of the
30   attributes being uncovered as part of the given pattern,
31

Application/Control Number: 10/798,070   **19/28**

1   plotting all the events arrived within the time period and including an attribute value

2   allocated to the primary attribute into the cross plot with the first display label indicating

3   the primary attribute, the position of the first display label of each event in the cross plot

4   being determined on the basis of the attribute value of the primary attribute of the event

5   and its arrival time,

6

7   plotting the all events arrived within the time period and being detected by means of the

8   pattern algorithm as part of the given pattern into the cross plot with the second display

9   label indicating the given pattern, the position of the second display label of each event in

10   the cross plot being determined by the mapping algorithm on the basis of the attribute

11   value of the attribute of the event being uncovered as part of the given pattern and its

12   arrival time, and

13

14   viewing a secondary attribute of said each event together with the primary attribute on

15   said display.

16

17   Thus claim 1 shows that the attribute are event attributes, and to show explicitly that it includes

18   "simultaneously monitoring various event attributes versus the arrival time of each the events,"

19   and to specifically add a step of "viewing a secondary attribute of said each event together with

20   the primary attribute on said display." This apparently more clearly distinguishes claim 1 from

21   the cited reference. Thus claim 1 and all claims that depend thereupon are allowable over Ma.

22

23

24   _Re Claims 2-3:_

25   _Ma further discloses selecting the new events within the specified time period and_

26   _plotting the new events within the shifted time period into the cross plot. See Figs. 6, 7, 9_

27   _and 10 in which events in the two time periods am drawn and the spikes are identified_

28   _arid the newly selected events are redrawn as determined by the data mining algorithm_

29   _for the time period during which the new events are retrieved. The database records the_

30   _attribute values and the arrival time of a new event. The pattern algorithm determines on_

31   _the basis of the recorded attribute values of event whether or not the newly arrived event_

32   _in the database and the newly retrieved event from the database includes an attribute_

33   _value of the primary attribute, for a certain host and event type, as determined the pattern_

34   _algorithm using the mapping mechanism for mapping a plurality of attributes including_

Application/Control Number: 10/798,070   20/28

1   *the primary attribute into an item for presentation, and the pattern algorithm also*
2   *determines if the newly arrived event, e.g., alarm, includes the attribute value for the*
3   *primary attribute, e.g., a certain host or a certain event type including SNMP request,*
4   *authentication failure, link up, link down, port up, port down, link down of host A, node*
5   *down of host B etc., shifting the x-axis of the cross plot for the new time period so that the*
6   *new time period being presented on the x-axis covers the arrival time of the event and*
7   *plotting the event arrived within the shifted time period into the cross plot with the first*
8   *display label indicating the primary attribute.*
9   *Ma discloses determining on the basis of the recorded attribute values of event*
10 *from the alarm log or the database whether or not the newly arrived event for the new*
11 *time period is part of the given pattern using the pattern algorithm on the basis of a*
12 *comparison of the attributes allocated to the given pattern, for example a composite*
13 *pattern of page 13, on the basis of a comparison analysis, and of the attribute assigned to*
14 *the arrived event wherein the newly arrived event are determined by the retrieval time*
15 *ranges and data ranges including the host names and types from the database. Ma thither*
16 *discloses determining if the newly arrived event includes an attribute value of the given*
17 *pattern including the mutual dependence measurement of an m-pattern adding the event*
18 *to the previous events being detected as part of the given pattern, and redrawing all the*
19 *events being associated with given pattern in the cross plot by updating the cross plot.*
20

21 In response, applicants respectfully state that exception is taken with the so called equivalencies

22 of elements in Claims 2 and 3 and the cited art. This is in regard to use of words in the claims

23 attributes, primary, events, display label etc. The present invention in 2 and 3 is not anticipated

24 by S. Ma, et al. As noted Ma's method is apparently that only one of the event attributes may be

25 plotted versus the arrival time of the events. Thus, the operators have to switch continuously

26 between the various event attributes to make sure that they do not miss a significant event

27 attribute or attributes or their simultaneous display. Ma is not concerned with the 'primary

28 attribute' nor for a plurality of event attributes, as in claims 2 and 3 which are allowable over Ma

29 in themselves and because each depends on allowable claim 1.

30

31   *Re Claims 4-5: Ma further discloses the third display label and the fourth display label*
32   *indicating the new patterns (See the three colored spikes in Fig. 6 and the four patterns in*
33   *Fig. 7).*
34   *Me discloses determining if the newly arrived event does not include an attribute value*
35   *of the given pattern, on the basis of the recorded attribute values of all previous arrived*
36   *events from the alarm logs or from the database, by means of the mining algorithm*
37   *'whether or not the newly arrived event is part of a new pattern on the basis of a*
38   *comparison (Page 13) of the attributes allocated to the new pattern and of the attributes*
39   *assigned to the arrived events. Ma discloses allocating a third display label to the events,*
40   *including the coloring of the new pattern, indicating the attribute values of the attributes*

Application/Control Number: 10/798,070   **21/28**

1 *being discovered as part of the new pattern wherein a large amount of patterns earl be*
2 *discovered by the mining algorithms. Ma discloses plotting the all events being detected*
3 *by means of the mining algorithm as part of the new pattern into the cross plot with the*
4 *third display label indicating the new pattern, the position of the third display label of*
5 *each event in the cross plot being determined by the mapping algorithm (Page 12 for the*
6 *mapping of the attributes into item and thereby determining the positions of the patterns*
7 *on the cross plot) on the basis of the attribute value of the attribute of the event (event*
8 *types, host names etc) being uncovered as part of the new pattern, such as SNMP request,*
9 *authentication failure, link up, link down, port up, port down, link down of host A, node*
10 *down of host B etc, and its arrival time in the database.*
11   *Ma discloses removing all the events including an attribute value allocated to the*
12 *primary attribute from the cross plot, if a primary attribute to be presented with its*
13 *attribute values on the y-axis of the cross plot is changed (if the mapping mechanism for*
14 *mapping a plurality of attributes including the host names and event types are changed),*
15 *allocating a fourth display label including SNMP request, authentication failure link up,*
16 *link down, port up, port down, link down of host A, node down of host B etc., to the events*
17 *indicating the attribute values of the new primary attribute (e.g., category attribute, event*
18 *type of data objects). Ma discloses plotting all the events arrived within the time period*
19 *as retrieved from the database and including an attribute value allocated to the new*
20 *primary attribute into the cross plot with the fourth display label, including SNMP*
21 *request, authentication failure, link up, link down, port up, port down, link down of host*
22 *A, node down of hosts etc indicating the new primary attribute, such as the host name*
23 *and event type, the position of the fourth display label of each event in the cross plot*
24 *being determined by the mapping mechanism in Page 12 on the basis of the attribute*
25 *value of the primary attribute of the event and its arrival time as determined by the*
26 *retrieval condition from the database.*
27

28 In response, applicants respectfully state that exception is taken with the so called equivalencies

29 of elements in Claims 4 and 5 and the cited art. This is in regard to use of words in the claims

30 attributes, primary, events, display label etc. The present invention in 4 and 5 is not anticipated

31 by S. Ma, et al. As noted, applicants respectfully state that the indicating of new patterns in Ma,

32 is not the steps of claim 4. Ma do not test as in claim 4, "if the newly arrived event does not

33 include an attribute value of the given pattern." Nor do Ma determine, "on the basis of the

34 recorded attribute values of all previous arrived events by means of the pattern algorithm whether

35 or not the newly arrived event is part of a new pattern on the basis of a comparison of the

36 attributes allocated to the new pattern and of the attributes assigned to the arrived events." Nor

37 do Ma test, "if the newly arrived event forms together with previous recorded events the new

38 pattern," Nor do Ma allocate, "a third display label to the events indicating the attribute values of

39 the attributes being uncovered as part of the new pattern." Certainly, Ma does apparently not

Application/Control Number: 10/798,070   22/28

1   perform the step of, "plotting the all events being detected by means of the pattern algorithm as

2   part of the new pattern into the cross plot with the third display label indicating the new pattern,

3   the position of the third display label of each event in the cross plot being determined by the

4   mapping algorithm on the basis of the attribute value of the attribute of the event being

5   uncovered as part of the new pattern and its arrival time.

6

7   Similarly, Ma are not concerned with a 'primary attribute nor with the step of claim 5, of

8   **removing all the events including an attribute value allocated to the primary attribute from**

9   **the cross plot,** if a primary attribute to be presented with its attribute values on the y-axis of the

10 cross plot is changed, allocating a fourth display label to the events indicating the attribute values

11 of the new primary attribute," nor with the step of, "plotting all the events arrived within the time

12 period and including an attribute value allocated to the new primary attribute into the cross plot

13 with the fourth display label indicating the new primary attribute, the position of the fourth

14 display label of each event in the cross plot being determined on the basis of the attribute value

15 of the primary attribute of the event and its arrival time," nor with the step of, "if a primary

16 attribute to be presented with its attribute values on the y-axis of the cross plot is changed,

17 allocating a fourth display label to the events indicating the attribute values of the new primary

18 attribute, and plotting all the events arrived within the time period and including an attribute

19 value allocated to the new primary attribute into the cross plot with the fourth display label

20 indicating the new primary attribute, the position of the fourth display label of each event in the

21 cross plot being determined on the basis of the attribute value of the primary attribute of the

22 event and its arrival time. Thus claims 4 and are allowable over Ma in themselves and because

23 each depends on allowable claim 1.

24

25   *Re Claim 6: Ma further discloses the operator selects the events to be plotted and*
26   *displaying textual and coloring information associated with the selected events on the*
27   *event display (Page 4 and Figs. 6, 7, 9-10).*
28   *Ma discloses plotting all attribute values, including the attributes such as event*
29   *type, link down, and host name, host A, in the patterns marked as the link down of host A,*
30   *node down of host B, recorded for an event, as retrieved from the database, with the*
31   *respective display label into the cross plot if the event is selected by an operator and*
32   *displaying textual information associated with the selected event on the event display.*
33

Application/Control Number: 10/798,070   **23/28**

1

 2   In response, applicants respectfully state that exception is taken with the so called equivalencies

3   of elements in Claim 6 and the cited art. This is in regard to use of words in the claims attributes,

4   primary, events, display label etc. The present invention in claim 6 is not anticipated by S. Ma,

5   et al. As noted, applicants respectfully state that Ma is not concerned with the test and step of

 6   claim 6 of, "plotting all attribute values recorded for an event with the respective display label

7   into the cross plot if the event is selected by an operator, and displaying textual information

8   associated with the selected event on the event display. Thus claim 6 is allowable over Ma for

9   itself and because it depends on allowable claim 1.

10

11   *Re Claim 7: Ma further discloses a pattern algorithm such as the data-mining algorithm*
12   *suitable to perform multi-attribute pattern recognition (Figs. 6, 7, 9-10).*
13   *Ma discloses the mining algorithm being suitable to perform multi-attribute*
14   *pattern recognition using the mapping mechanism (Page 12) and the pattern*
15   *comparisons/matching (Page 13).*
16

17   In response, applicants respectfully state that exception is taken with the so called equivalencies

18   of elements in Claim 7 and the cited art. This is in regard to use of words in the claims attributes,

19   primary, events, display label etc. The present invention in claim 7 is not anticipated by S. Ma,

20   There is apparently no indication that Ma is concerned with multi-attribute pattern recognition or

21   even any pattern recognition as in claim 7. Being allegedly suitable is indeed not an anticipation

22   of the invention in claim 7. Thus claim 7 is allowable over Ma for itself and because it depends

23   on allowable claim 1.

24

25   *Re Claim 8: Ma further discloses using color such as Red and Green to color the pattern*
26   *Spikes and Pattern 1, Pattern 2, Pattern 3, Pattern 4 for specific mark layouts (Figs. 6, 7,*
27   *9-10).*
28   *Ma discloses each display label includes different colors marking the events.*
29

30   In response, applicants respectfully state that claim 7 is allowable over Ma because it depends on

31   allowable claim 1.

32

33   *Re Claim 9: Ma further discloses all events being uncovered as part of the pattern being*
34   *clustered by the display label such as Red Spikes, Green Spikes (Figs. 6, 7 and 9-10).*

Application/Control Number: 10/798,070   **24/28**

1   *Ma discloses all events being discovered as part of the pattern as clustered by the*
2   *different labels including Red Spikes and Green Spikes to indicate one of the plurality of*
3   *events such as SNMP request, authentication failure, link up, link down, port up, port*
4   *down, link down of host A, node down of host B etc indicating the new primary attribute.*
5

6   In response, applicants respectfully state that there is apparently no indication that Ma is at all

7   concerned with clusters or clustering as in claim 9. Thus claim 9 is allowable over Ma for itself

8   and because it depends on allowable claim 1.

9

10   *Re Claim 10: Ma further discloses a data mining algorithm and GUI (Page 14). Ma*
11   *discloses the mining algorithm carrying the steps as recited in the claim 1.*
12

13   In response, applicants respectfully state that the response to claim 1 is appropriate to claim 10

14   which depends thereupon. The program code is the that of claim 1, which is not anticipated by

15   Ma. Thus claim 10 is allowable over Ma for itself and because it depends on allowable claim 1.

16

17   *Re Claim 11: Ma further discloses the program code being stored on data carrier (see*
18   *page 5). Data carrier is inherent within the computer embodiment of Page 5.*
19

20   In response, applicants respectfully state that exception is taken with the stated inherentcy. There

21   is apparently no indication that Ma discloses or is concerned with a data carrier as in claim 11.

22   Thus claim 11 is allowable over Ma for itself and because it depends on allowable claim 1.

23

24   *Re Claim 12: Ma further discloses an event visualization device for monitoring events in*
25   *a computer network (Page 3). The cited reference teach mapping a plurality of data*
26   *attributes to item to identify correlations across different hosts and event types by using*
27   *the mapping that maps the pair of event type and host name to item and leaves key empty.*
28   *See Page 11. Moreover, the cited reference in Page 1, second paragraph, explicitly*
29   *teaches the attribute values, see the last paragraph of Page 6 and the first and second*
30   *paragraphs of Page 8, the last paragraph of Page 12, and the real data set collected*
31   *from a production computer network containing thousands of managed nodes including*
32   *routers, hubs and servers are described in the last paragraph of page 3 and identifying*
33   *unknown event patterns that can be used for real-time monitoring is described in the*
34   *second paragraph of page 3.*
35

36   In response, applicants respectfully state that exception is taken with the so called equivalencies

37   of elements in Claim 6 and the cited art. This is in regard to use of words in the claims attributes,

Application/Control Number: 10/798,070   **25/28**

1   primary, events, display label etc., and an event visualization device. The present invention in

2   claim 12 is not anticipated by S. Ma. The response to claim 1 is appropriate to claim 12, which

3   depends thereupon. The device is for performing the steps of claim 1, which is not anticipated by

4   Ma. Thus claim 12 is allowable over Ma for itself and because it depends on allowable claim 1.

5
6   *Re Claims 13-15: Ma further discloses an implementation of the Event Miner algorithm*
7   *on the computer (Page 4-5).*
8
9   In response, applicants respectfully state that exception is taken with the so called equivalencies

10   of elements in Claims 13-16 and the cited art. This is in regard to use of words in the claims

11   attributes, primary, events, display label etc. The present invention in claim 13-15 are not

12   anticipated by S. Ma. The response to claim 1 is appropriate to claim 13 and 15, which depends

13   thereupon. Claim 14 is amended to be an independent claim of the Beauregard type, with all the

14   elements of claim 1. The implementations are for performing the steps of claim 1, which is not

15   anticipated by Ma. Thus claims 13-15 are allowable over Ma for itself and because it depends on,

16   or has the matter, of allowable claim 1.

17

18   *Claim 16: The claim 16 is subject to the same rationale of rejection set forth in the*
19   *claims 2-4.*
20

21   In response, applicants respectfully state that as with claims 2-4, exception is taken with the so

22   called equivalencies of elements in Claim 16 and the cited art. This is in regard to use of words

23   in the claims attributes, primary, events, display label etc. There is apparently no indication that

24   MA performs the added steps of claim 16. The present invention in claim 16 is not anticipated

25   by S. Ma. The response to claim 1 is appropriate to claim 16, which depends thereupon. The

26   method is for performing more steps over the steps of claim 1, which is not anticipated by Ma.

27   Thus claim 16 is allowable over Ma for itself and because it depends on allowable claim 1.

28

29   *Claim 17: The claim 17 is subject to the same rationale of rejection set forth in the claim*
30   *5.*
31

32   In response, applicants respectfully state that as with claim 5 exception is taken with the so called

33   equivalencies of elements in Claim 17 and the cited art. This is in regard to use of words in the

Application/Control Number: 10/798,070   **26/28**

1   claims attributes, primary, events, display label etc. There is apparently no indication that MA

2   performs the added steps of claim 17. The present invention in claim 17 is not anticipated by S.

3   Ma. The response to claim 1 is appropriate to claim 17, which depends thereupon. The method

4   is for performing more steps over the steps of claim 16, which is not anticipated by Ma. Thus

5   claim 17 is allowable over Ma for itself and because it depends on allowable claim 1.

6

7   *Claim 18:* *The claim 18 is subject to the same rationale of rejection set forth in the claims*
8   *2-4.*
9
10

11   In response, applicants respectfully state that as with claims 2-4, exception is taken with the so

12   called equivalencies of elements in Claim 18 and the cited art. This is in regard to use of words

13   in the claims attributes, primary, events, display label etc. There is apparently no indication that

14   Ma has the added elements of claim 18. The present invention in claim 18 is not anticipated by

15   S. Ma. The response to claim 1 is appropriate to claim 18, which depends thereupon. The device

16   is for more elements than claim 5, which is not anticipated by Ma. Thus claim 18 is allowable

17   over Ma for itself and because it depends on allowable claim 1.

18

19   *Claim 19:* *The claim 19 is subject to the same rationale of rejection set forth in the claim*
20   *5.*
21

22   In response, applicants respectfully state that as with claim 5 exception is taken with the so called

23   equivalencies of elements in Claim 19 and the cited art. This is in regard to use of words in the

24   claims attributes, primary, events, display label etc. There is apparently no indication that Ma

25   performs the added steps of claim 19 has the added elements of claim 189. The response to

26   claim 1 is appropriate to claim 17, which depends thereupon. The device is for more elements

27   than claim 5, which is not anticipated by Ma. Thus claim 17 is allowable over Ma for itself and

28   because it depends on allowable claim 1.

29

30   *Claim 20:* *The claim 20 is subject to the same rationale of rejection set forth in the claim*
31   *11.*
32

Application/Control Number: 10/798,070   **27/28**

1   In response, applicants respectfully state that claim 20 is amended to be an independent claim for

2   an article of manufacture, without introducing new matter. As with claim 1, claim 20 shows that

3   the attribute are event attributes, and to show explicitly that it includes "means for

4   simultaneously monitoring various event attributes versus the arrival time of each the events,"

5   and to specifically include "means for viewing a secondary attribute of said each event together

6   with the primary attribute on said display." This apparently more clearly distinguishes claim 1

7   and 20, from the cited reference. Thus claim 1 and all claims that depend thereupon including

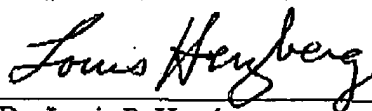8   20, are allowable over Ma.

9

10   Claim 14 is amended to be an independent claim of the Beauregard type, with all the elements of

11   claim 1. Thus it is allowable over the cited art.

12

13   It is anticipated that this amendment brings the application to allowance of claims 1-20.

14   Favorable action is respectfully solicited. In the unlikely event that any claim remains rejected,

15   please contact the undersigned by phone in order to discuss the application.

16

17   Please charge any fee necessary to enter this paper to deposit account 50-0510.

18
19   Respectfully submitted,
20
21
22   By: _____
23   Dr. Louis P. Herzberg
24   Reg. No. 41,500
25   Voice Tel. (845) 352-3194
26   Fax. (914) 945-3281
27
28   3 Cloverdale Lane
29   Monsey, NY 10952
30
31   Customer Number: 54856

Application/Control Number: 10/798,070   **28/28**